



## DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND

P.O. BOX 12798

FORT HUACHUCA, ARIZONA 85670-2798

IN REPLY  
REFER TO: Networks and Transport Division (JTE)

6 December 2004

### MEMORANDUM FOR DISTRIBUTION

**SUBJECT:** Special Interoperability Test Certification of the ION Networks ION Secure™ PRIISMS with Software Release 2.2.1 build 9 and ION Secure™ 5500 with Software Release 5.1.9 build 5 (Firmware 5.1.8)

**References:** (a) DOD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004  
(b) CJCSI 6212.01C, "Interoperability and Supportability of Information Technology and National Security Systems," 20 November 2003

1. References (a) and (b) establish the Defense Information Systems Agency, Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification. Additional references are provided in enclosure 1.
2. ION Networks ION Secure™ PRIISMS with Software Release 2.2.1 build 9 and ION Secure™ 5500 with Software Release 5.1.9 build 5 (Firmware 5.1.8), hereinafter referred to as the system under test (SUT), meet the interface and functional requirements, and are certified for joint use within the Defense Switched Network (DSN). The SUT met the interface and functional requirements for customer premise equipment devices set forth in appendix 7 of reference (c). Although the SUT consists of the ION Secure™ PRIISMS and the ION Secure™ 5500, each of these components is independently certified for joint use with the DSN. Testing was conducted using test procedures derived from reference (d). This certification expires upon changes that affect interoperability, but no later than three years from the date of this memorandum.
3. This certification is based on interoperability testing conducted by JITC at the Global Information Grid Network Test Facility, Fort Huachuca, AZ, from 19 through 20 May 2004, analysis of GSCR appendix 7 requirements, which were approved on 1 July 2004, and approval of vendor Letters of Compliance completed on 4 August 2004. The Certification Testing Summary (enclosure 2) documents the test results and describes the test configuration. Users should verify interoperability before deploying the SUT in an environment that varies significantly from that described.
4. The Functional Requirements used to evaluate the interoperability of the SUT and the interoperability statuses are indicated in table 1.

**Table 1. SUT Functional Requirements and Interoperability Status**

Interfaces	Critical	Certified	Functional Requirements	Met	GSCR Paragraph																										
Ethernet TCP/IP  IEEE 802.3 (10BaseT) IEEE 802.3.u (100BaseTX)	No	Yes	Network Management (C)	Met	A.7.5																										
ITU V.35 Serial	No	Yes	ITU V.35 (C)	Met	A7.5																										
EIA-232 Serial	No	Yes	ANSI/TIA/EIA-232-F (C)	Met	A7.5																										
2-Wire Analog (GR-506-CORE)	No <sup>1</sup>	Yes	MLPP in accordance with GSCR, Section 3 (C)	Met	A7.5																										
			MLPP Precedence call alerting (C)	Not Tested	A7.5																										
			FCC Part 15/Part 68 (R)	Met	A7.5																										
			Auto answer ring interval (C)	Not Tested	A7.5																										
			DTMF outpulsing (C)	Met	A7.5, 5.4.1, 5.4.2																										
			JTA compliance as applicable (R)	Met	A7.5																										
			Routine precedence only in accordance with GSCR, Section 3.3 (R)	Met	A7.5																										
			ANSI/TIA/EIA-470-B (R: Analog only)	Met	A7.5.1																										
Security in accordance with DITSCAP (R) <sup>2</sup>	Met	A7.6.5																													
<b>Legend:</b>																															
<table border="0"> <tr> <td>10BaseT - 10 Mbps (Baseband Operation, Twisted Pair) Ethernet</td> <td>IEEE - Institute of Electrical and Electronics Engineers, Inc.</td> </tr> <tr> <td>100BaseTX - 100 Mbps Ethernet over Category 5 Twisted Pair Copper</td> <td>ISDN - Integrated Services Digital Network</td> </tr> <tr> <td>ANSI - American National Standards Institute</td> <td>IT - Information Technology</td> </tr> <tr> <td>BRI - Basic Rate Interface</td> <td>ITU - International Telecommunication Union</td> </tr> <tr> <td>C - Conditional</td> <td>JTA - Joint Technical Architecture</td> </tr> <tr> <td>DISA - Defense Information Systems Agency</td> <td>Mbps - Megabits per second</td> </tr> <tr> <td>DITSCAP - DOD IT Security Certification &amp; Accreditation Process</td> <td>MLPP - Multi-Level Precedence and Preemption</td> </tr> <tr> <td>DOD - Department of Defense</td> <td>PCM-24 - Pulse Code Modulation - 24 Channels</td> </tr> <tr> <td>DTMF - Dual Tone Multi-Frequency</td> <td>PCM-30 - Pulse Code Modulation - 30 Channels</td> </tr> <tr> <td>EIA - Electronic Industries Alliance</td> <td>R - Required</td> </tr> <tr> <td>FCC - Federal Communications Commission</td> <td>SUT - System Under Test</td> </tr> <tr> <td>GR - Generic Requirement</td> <td>TCP/IP - Transmission Control Protocol/Internet Protocol</td> </tr> <tr> <td>GSCR - Generic Switching Center Requirements</td> <td>TIA - Telecommunications Industry Association</td> </tr> </table>						10BaseT - 10 Mbps (Baseband Operation, Twisted Pair) Ethernet	IEEE - Institute of Electrical and Electronics Engineers, Inc.	100BaseTX - 100 Mbps Ethernet over Category 5 Twisted Pair Copper	ISDN - Integrated Services Digital Network	ANSI - American National Standards Institute	IT - Information Technology	BRI - Basic Rate Interface	ITU - International Telecommunication Union	C - Conditional	JTA - Joint Technical Architecture	DISA - Defense Information Systems Agency	Mbps - Megabits per second	DITSCAP - DOD IT Security Certification & Accreditation Process	MLPP - Multi-Level Precedence and Preemption	DOD - Department of Defense	PCM-24 - Pulse Code Modulation - 24 Channels	DTMF - Dual Tone Multi-Frequency	PCM-30 - Pulse Code Modulation - 30 Channels	EIA - Electronic Industries Alliance	R - Required	FCC - Federal Communications Commission	SUT - System Under Test	GR - Generic Requirement	TCP/IP - Transmission Control Protocol/Internet Protocol	GSCR - Generic Switching Center Requirements	TIA - Telecommunications Industry Association
10BaseT - 10 Mbps (Baseband Operation, Twisted Pair) Ethernet	IEEE - Institute of Electrical and Electronics Engineers, Inc.																														
100BaseTX - 100 Mbps Ethernet over Category 5 Twisted Pair Copper	ISDN - Integrated Services Digital Network																														
ANSI - American National Standards Institute	IT - Information Technology																														
BRI - Basic Rate Interface	ITU - International Telecommunication Union																														
C - Conditional	JTA - Joint Technical Architecture																														
DISA - Defense Information Systems Agency	Mbps - Megabits per second																														
DITSCAP - DOD IT Security Certification & Accreditation Process	MLPP - Multi-Level Precedence and Preemption																														
DOD - Department of Defense	PCM-24 - Pulse Code Modulation - 24 Channels																														
DTMF - Dual Tone Multi-Frequency	PCM-30 - Pulse Code Modulation - 30 Channels																														
EIA - Electronic Industries Alliance	R - Required																														
FCC - Federal Communications Commission	SUT - System Under Test																														
GR - Generic Requirement	TCP/IP - Transmission Control Protocol/Internet Protocol																														
GSCR - Generic Switching Center Requirements	TIA - Telecommunications Industry Association																														
<b>Notes:</b>																															
1 The Automated Receiving Device requirements can be met via one of the following interfaces: 2-Wire Analog, 2- or 4-Wire Digital Proprietary, ISDN BRI, PCM-24, or PCM-30.																															
2 DITSCAP information assurance testing is accomplished via DISA-led Information Assurance test teams.																															

5. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/.gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet), or <http://199.208.204.125> (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>.

JITC Memo, JTE, ION Networks ION Secure™ PRIISMS with Software Release 2.2.1 build 9 and ION Secure™ 5500 with Software Release 5.1.9 build 5 (Firmware 5.1.8)

6. The JITC point of contact is Mr. Michael Napier, DSN 879-6787, commercial (520) 538-6787, FAX DSN 879-4347, or e-mail to [napierm@fhu.disa.mil](mailto:napierm@fhu.disa.mil).

FOR THE COMMANDER:

2 Enclosures a/s

LESLIE CLAUDIO  
Chief  
Networks and Transport Division

Distribution:

Joint Staff J6I, Room-1E565, Pentagon, Washington, DC 20318-6000

Joint Interoperability Test Command, Washington Operations Division, NSWC, ATTN: JT1,  
Building 900, 101 Strauss Avenue, Indian Head, MD 20640-5035

Defense Information Systems Agency, GIG Enterprise Services Engineering Directorate,  
NETCENTRICITY, REQUIREMENTS, ANALYSIS & ASSESSMENTS BRANCH, ATTN:  
GE333, Rm. 244, 5600 Columbia Pike, Falls Church, VA 22041-2770

Defense Information Systems Agency, GIG-Combat Support Directorate, DSN SYSTEMS  
MANAGEMENT BRANCH, ATTN: GS235, Rm. 5W248A, 5275 Leesburg Pike, Falls  
Church, VA 22041

Office of Chief of Naval Operations (N61C22), CNON6/7, 2000 Navy Pentagon, Washington,  
DC 20350

Headquarters US Air Force, AF/XICC, 1250 Pentagon, Washington, DC 20330-1250

Department of the Army, Office of the Secretary of the Army, G-6/ASA (ALT), ATTN:  
ASAALT (SAAL-SSI), 103 Army Pentagon, Washington, DC 20310-0103

US Marine Corp (C4ISR), MARCORSSYSCOM, 2200 Lester Street, Quantico, VA 22134

DOT&E, Strategic and C3I Systems, 1700 Defense Pentagon, Washington, DC 20301-1700

US Coast Guard, COMDT/G-SCE (C4), 2100 2nd Street SW, Washington, DC 20593

Office of Assistant Secretary of Defense, OASD(NII)/DoD CIO, Crystal Mall 3, 7<sup>th</sup> Floor, Suite  
700, 1931 Jefferson-Davis Hwy, Arlington, VA 22202

Office of Under Secretary of Defense, OUSD(AT&L), Room 3E144, 3070 Defense Pentagon,  
Washington, DC 20301

US Joint Forces Command, J6I, C4 Plans and Policy, 1562 Mitscher Ave, Norfolk, VA 23551-  
2488

Defense Intelligence Agency, ATTN: DS-CIO, Bldg 6000, Bolling AFB, Washington, DC  
20340-3342

National Security Agency, ATTN: DT, Suite 6496, 9800 Savage Road, Fort Meade, MD  
20755-6496

Commander, Defense Information Systems Agency (DISA), ATTN: GS23 (Mr. Osman), Room  
5w23, 5275 Leesburg Pike (RTE 7), Falls Church, VA 22041

## **ADDITIONAL REFERENCES**

- (c) Defense Information Systems Agency, "Department of Defense Voice Networks Generic Switching Center Requirements (GSCR)," 8 September 2003
- (d) Joint Interoperability Test Command, "Defense Switched Network Generic Switch Test Plan (GSTP)," 23 April 2004

## CERTIFICATION TESTING SUMMARY

**1. SYSTEM TITLE.** ION Networks ION Secure™ PRIISMS with Software Release 2.2.1 build 9 and ION Secure™ 5500 with Software Release 5.1.9 build 5 (Firmware 5.1.8), hereinafter referred to as the system under test (SUT).

**2. PROPONENT.** Defense Information Systems Agency (DISA).

**3. PROGRAM MANAGER.** Mr. Howard Osman, GS23, Room 5W23, 5275 Leesburg Pike, Falls Church, VA 22041, e-mail: Osmanh@ncr.disa.mil.

**4. TESTER.** Joint Interoperability Test Command (JITC), Ft. Huachuca, AZ.

**5. SYSTEM UNDER TEST DESCRIPTION.** ION Secure™ solutions protect administrative access points through the flexible definition and stringent enforcement of access, authentication, and authorization privileges. ION Secure™ solutions provide administrative functionality to ensure secure network connectivity, and complete audit data for post-breach analysis with support for a wide range of critical enterprise devices and applications. Further descriptions of the ION Networks' ION Secure™ PRIISMS Administrator Portal and the ION Secure™ 5500 follow:

**a. ION Networks' ION Secure™ PRIISMS.** PRIISMS is a single sign-on, multi-factor authentication portal providing encrypted dial-up or secure Internet Protocol (IP) tunnel connectivity from a local or remote workstation through ION Secure™ appliances to a wide range of end devices. PRIISMS delivers a scalable and auditable gateway for all administrative-class users. The PRIISMS Administrator Portal provides a centralized platform for administrative security policy definition and control. PRIISMS provides scalable functionality to define and manage security for the enterprise network. PRIISMS forms a secure and auditable gateway for all administrator channel access, ensuring protection of critical data. PRIISMS provides the following features and functionality:

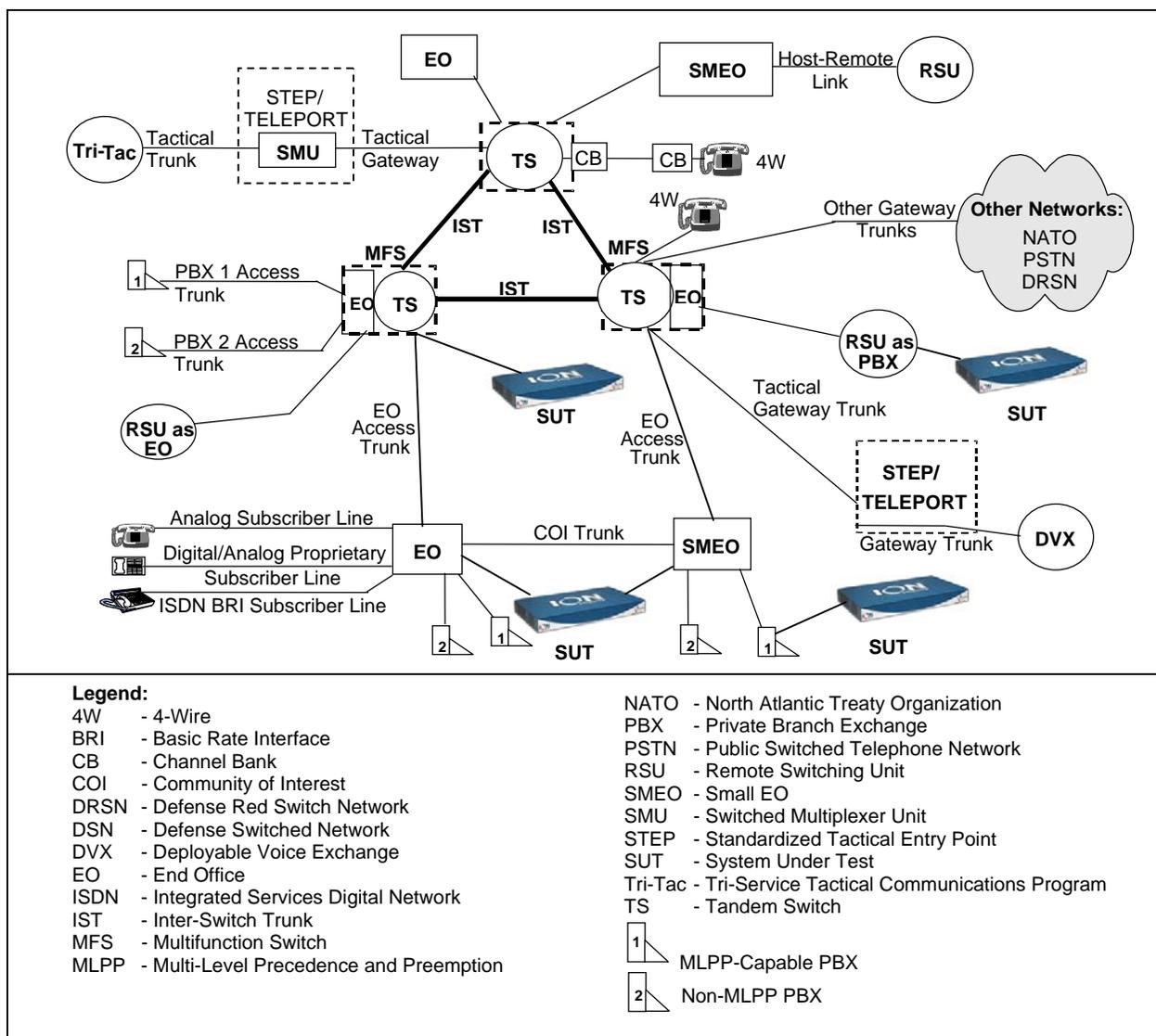
- Secure Access via Virtual Private Network (VPN) and Virtual Private Data Network
- Single Sign-On
- Multi-factor authentication
- Multi-level authorization
- Real-time event definition and notification
- Policy definition and enforcement

**b. ION Secure™ 5500.** The ION Secure™ 5500 security appliance supports between 4 and 28 console ports to secure physically connected devices, and a network interface to secure up to 64 IP-connected devices or applications. The ION Secure 5500 also provides additional security through its ability to connect to ION Secure™ PRIISMS via an encrypted IP Security VPN tunnel.

The ION Secure 5500 appliance has over 30 Megabits of memory to store keystroke logging of administrative sessions. These logs may be transferred to ION Secure™ PRIISMS for centralized storage and viewing, and provide the foundation for routine operational reviews and post-breach analysis.

The ION Secure 5500 uses only a single-rack unit. By utilizing the capabilities of the ION Secure™ 5500 security appliance, complex enterprise networks can be protected from malicious, administrative channel attack from a 'trusted' third-party vendor or a simple, inexperienced user error from an internal administrator.

**6. OPERATIONAL ARCHITECTURE.** The Generic Switching Center Requirements (GSCR) Defense Switched Network (DSN) architecture in figure 2-1 depicts the relationship of the SUT to the DSN switches.



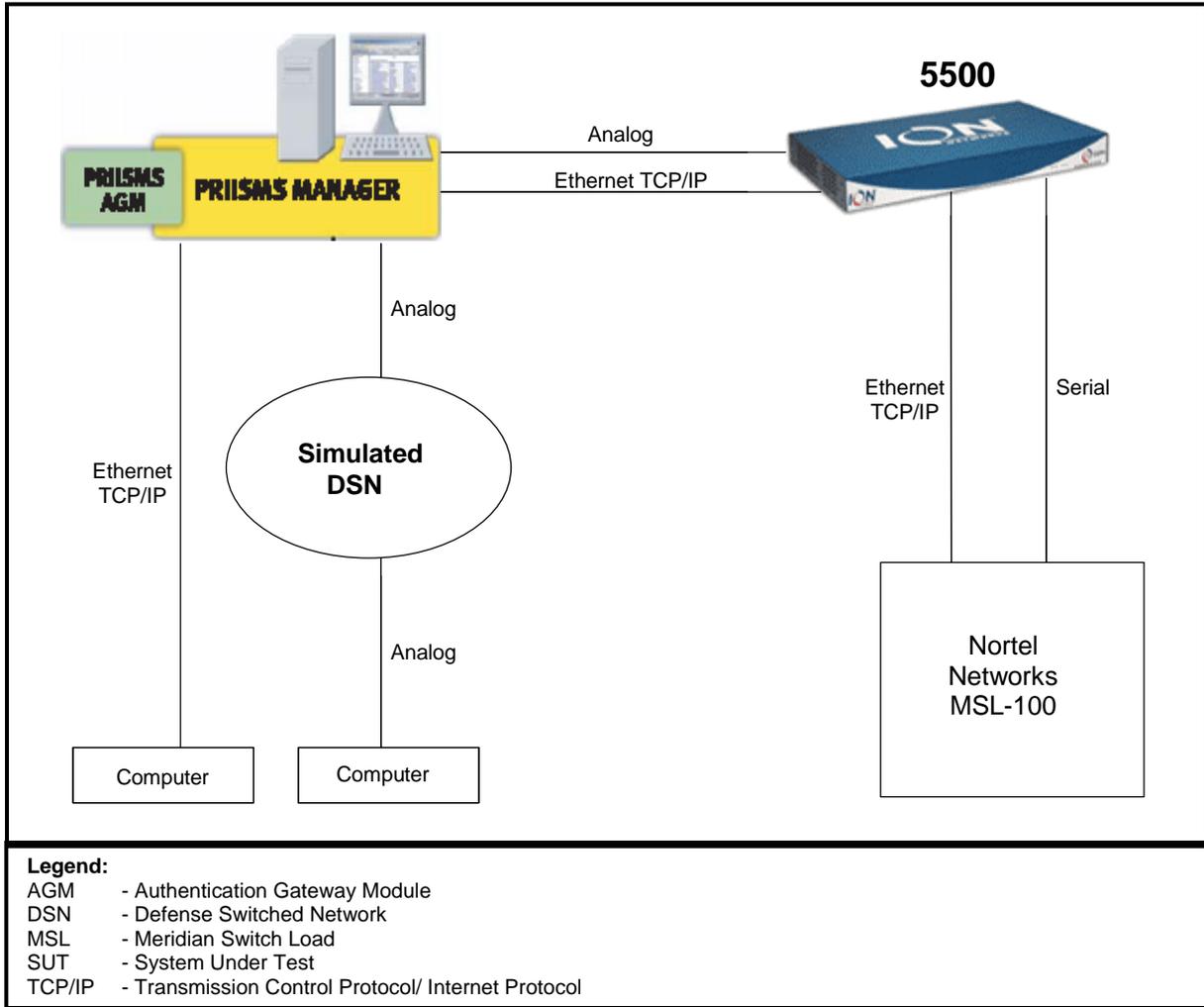
**Figure 2-1. DSN Architecture**

**7. REQUIRED SYSTEM INTERFACES.** Requirements specific to the SUT and interoperability results are listed in table 2-1. These requirements are derived from GSCR Interface and Functional Requirements (FRs) verified through JITC testing and/or vendor submission of Letter(s) of Compliance.

**Table 2-1. SUT Functional Requirements and Interoperability Status**

Interfaces	Critical	Certified	Functional Requirements	Met	GSCR Paragraph
Ethernet TCP/IP  IEEE 802.3 (10BaseT) IEEE 802.3.u (100BaseTX)	No	Yes	Network Management (C)	Met	A.7.5
ITU V.35 Serial	No	Yes	ITU V.35 (C)	Met	A7.5
EIA-232 Serial	No	Yes	ANSI/TIA/EIA-232-F (C)	Met	A7.5
2-Wire Analog (GR-506-CORE)	No <sup>1</sup>	Yes	MLPP in accordance with GSCR, Section 3 (C)	Met	A7.5
			MLPP Precedence call alerting (C)	Not Tested	A7.5
			FCC Part 15/Part 68 (R)	Met	A7.5
			Auto answer ring interval (C)	Not Tested	A7.5
			DTMF outpulsing (C)	Met	A7.5, 5.4.1, 5.4.2
			JTA compliance as applicable (R)	Met	A7.5
			Routine precedence only in accordance with GSCR, Section 3.3 (R)	Met	A7.5
			ANSI/TIA/EIA-470-B (R: Analog only)	Met	A7.5.1
Security in accordance with DITSCAP (R) <sup>2</sup>	Met	A7.6.5			
<b>Legend:</b>					
10BaseT	- 10 Mbps (Baseband Operation, Twisted Pair) Ethernet	IEEE	- Institute of Electrical and Electronics Engineers, Inc.		
100BaseTX	- 100 Mbps Ethernet over Category 5 Twisted Pair Copper	ISDN	- Integrated Services Digital Network		
ANSI	- American National Standards Institute	IT	- Information Technology		
BRI	- Basic Rate Interface	ITU	- International Telecommunication Union		
C	- Conditional	JTA	- Joint Technical Architecture		
DISA	- Defense Information Systems Agency	Mbps	- Megabits per second		
DITSCAP	- DOD IT Security Certification & Accreditation Process	MLPP	- Multi-Level Precedence and Preemption		
DOD	- Department of Defense	PCM-24	- Pulse Code Modulation - 24 Channels		
DTMF	- Dual Tone Multi-Frequency	PCM-30	- Pulse Code Modulation - 30 Channels		
EIA	- Electronic Industries Alliance	R	- Required		
FCC	- Federal Communications Commission	SUT	- System Under Test		
GR	- Generic Requirement	TCP/IP	- Transmission Control Protocol/Internet Protocol		
GSCR	- Generic Switching Center Requirements	TIA	- Telecommunications Industry Association		
<b>Notes:</b>					
1 The Automated Receiving Device requirements can be met via one of the following interfaces: 2-Wire Analog, 2- or 4-Wire Digital Proprietary, ISDN BRI, PCM-24, or PCM-30.					
2 DITSCAP information assurance testing is accomplished via DISA-led Information Assurance test teams.					

**8. TEST NETWORK DESCRIPTION.** The SUT was tested at JITC's Global Information Grid Network Test Facility in a manner and configuration similar to that of the DSN operational environment. The test configuration depicted in figure 2-2 was used to test the system's interface functions and features.



**Figure 2-2. SUT Test Configuration**

**9. SYSTEM CONFIGURATIONS.** The tested system configurations are shown in table 2-2.

**Table 2-2. Tested System Configurations**

System Name	Software Release
Nortel Networks MSL-100	SE06
<b>SUT</b>	
ION Secure™ PRIISMS	2.2.1 build 9
ION Secure™ 5500	5.1.9 build 5 (Firmware 5.1.8)
PC	Dell 7100 Server with Windows 2000 SP 4
<b>Legend:</b> MSL - Meridian Switching Load                      SU - Software Update PC - Personal Computer                                SUT - System Under Test SE - Succession Enterprise SP - Service Pack	

**10. TEST LIMITATIONS.** None.

**11. TEST RESULTS**

**a. Discussion.** The SUT basic secure functions were tested using the test configuration shown in figure 2-2. The various interface combinations and their respective test results are shown in table 2-3. Testing was conducted to ensure that the SUT encryption was transparent to the established data calls and, when released, they were properly returned to an idle state ready for the next data call attempt.

**Table 2-3. Interface Combinations**

Connection to ION Secure™ PRIISMS	Connection to ION Secure™ 5500	Connection to DSN Switch	Test Results
Analog	TCP/IP	TCP/IP	Passed
Analog	TCP/IP	Serial	Passed
TCP/IP	TCP/IP	TCP/IP	Passed
TCP/IP	TCP/IP	Serial	Passed
TCP/IP	Analog	TCP/IP	Passed
TCP/IP	Analog	Serial	Passed
<b>Legend:</b> DSN - Defense Switched Network TM - Trade Mark TCP/IP - Transmission Control Protocol/Internet Protocol			

**b. Lessons Learned**

(1) For connections leaving the SUT, the control characters in the *end-point connections and buffer settings* have to be disabled. Otherwise, the SUT will not pass Control-Break messages to the next device.

(2) The PRIISMS Network Interface Card must be connected to the network in order for the software to operate properly.

**c. Test Summary.** The SUT met the critical interoperability requirements for a customer premise device for the interfaces shown in table 2-1, as set forth in reference (c), and is certified for joint use within the DSN.

**12. TESTS AND ANALYSIS REPORT.** No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet), or <http://199.208.204.125> (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>.